REMARKS

Applicants respectfully request favorable reconsideration of this application, as amended.

Claims 19, 21, 23-36 and 39 are pending. By this amendment, Claims 19, 33, and 39 have been amended to more particularly recite subject matter which Applicants regard as their invention, as discussed in detail below. Claim 36 has also been amended for consistency. Claims 1-18, 20, 22, 37-38, and 40 were previously cancelled without prejudice or disclaimer.

In the Office Action, Claims 19, 21, 23-36 and 39 were rejected under 35 U.S.C § 103(a) over Hopkins in combination with Aoki.

Without acceding to the rejection, Claim 19 has been amended to recite, *inter alia*, means for storing personalized data (z, Kz) identifying any one individual member (M) of a group (G), in which the group signature device is associated to the one individual member (M) of the group (G);

means for storing a predefined private signature key (SK) common to all members of the group (G);

encryption means (B3) for producing a single encrypted text (C), intended to be associated with the message (m), using the personalized data (z, Kz) of one individual member (M) only;

signing means (B6) which enables the one individual member (M) to produce the group signature (S) on behalf of the group (G) using the stored predefined private signature key (SK) common to all group members, in which only the message to be signed (m) and the single encrypted text (C) produced using the personalized data (z, Kz) of the one individual member (M) are used to produce the group signature (S).

Support is provided at, for example, page 1, lines 9-13; and page 13, lines 22-24 of Applicants' disclosure. It is apparent that the applied references do not teach or suggest at least these features.

For example, the primary reference, Hopkins, is not seen as teaching or suggesting, at minimum, means (B3) for producing a single encrypted text (C), intended to be associated with the message (m), using the personalized data (z, Kz) of one individual member (M) only, as recited in Claim 19. Nor does the Office Action rely on Hopkins for such teaching.

However, it is alleged that Hopkins deficiencies in this regard are cured by the teachings found in secondary reference Aoki. Applicants respectfully disagree.

Secondary reference Aoki is directed to a public key encryption and key management system that uses a "composite lock." *See* Aoki, Abstract; and col. 8, lines 19-22. For example, Aoki is understood as teaching a group secret key S_G that is encrypted using the individual public keys of all members of the group, so that a group lock or composite lock can be provided. Aoki, col. 7, lines 1-5. Thus, the cited portion of Aoki is not understood as teaching that Aoki's P_{Mi} element is generated by a device associated to the individual member of the group. Aoki, col. 3, lines 2-19; and FIG. 8.

Furthermore, neither Hopkins nor Aoki is seen as teaching or suggesting producing a single encrypted text (C) intended to be associated with the message (m). In contrast, Hopkins and Aoki are each seen as teaching producing multiple encrypted texts. For example, the cited portion of Hopkins relied on by Office Action as allegedly teaching or suggesting Applicants' signing means (B6) for producing the group signature (S) with a private signature key (SK) clearly discloses that the key

used by the individual to generate a partial signature in Hopkins is an individual private key, and that "[t]he partial digital signatures are then combined mathematically to create a group digital signature." *See* Hopkins, col. 5, lines 22-31; and col. 11, lines 40-55 (underlines added).

Furthermore, the cited portion of Aoki is understood as teaching that Aoki's P_{Mi} element is used to produce and modify a group lock comprising all of the P_{Mi} elements for all of the members of the group. Aoki, col. 3, lines 2-19; and FIG. 8.

Accordingly, neither Hopkins nor Aoki is seen as teaching or suggesting encryption means (B3) for producing a single encrypted text (C), intended to be associated with the message (m), using the personalized data (z, Kz) of one individual member (M) only; and signing means (B6) which enables the one individual member (M) to produce the group signature (S) on behalf of the group (G) using the stored predefined private signature key (SK) common to all group members, in which only the message to be signed (m) and the single encrypted text (C) produced using the personalized data (z, Kz) of the one individual member (M) are used to produce the group signature (S), as recited in Claim 19.

Therefore, Applicants respectfully submit that Claim 19 distinguishes patentably from the applied references.

Claims 33 and 39 have been similarly amended. Accordingly, Applicants respectfully submit that Claims 33 and 39 also distinguish patentably from the applied reference for at least the reasons discussed above with respect to Claim 19.

The dependent Claims 21, 23-32, and 34-36 are also believed to be patentable based on their dependence from Claims 19 and 33, as well as due to the additional features recited in Claims 21, 23-32, and 34-36.

Therefore, Applicants respectfully submit that this application is in condition for allowance. A prompt Notice of Allowance is respectfully requested.

Should the Examiner believe that any further action is necessary to place this application in better form for allowance, the Examiner is invited to contact Applicants' representative at the telephone number listed below.

The Commissioner is hereby authorized to charge to Deposit Account No. 50-1165 (T2678-9156US01) any fees under 37 C.F.R. §§ 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any extension of time is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

Respectfully submitted,

Date: August 31, 2009

By: _____
Eric G. King
Reg. No. 42,736

Miles & Stockbridge, P.C.
1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
Telephone: (703) 610-8647